



New Hampshire Information & Analysis Center

COVID-19 Weekly Report

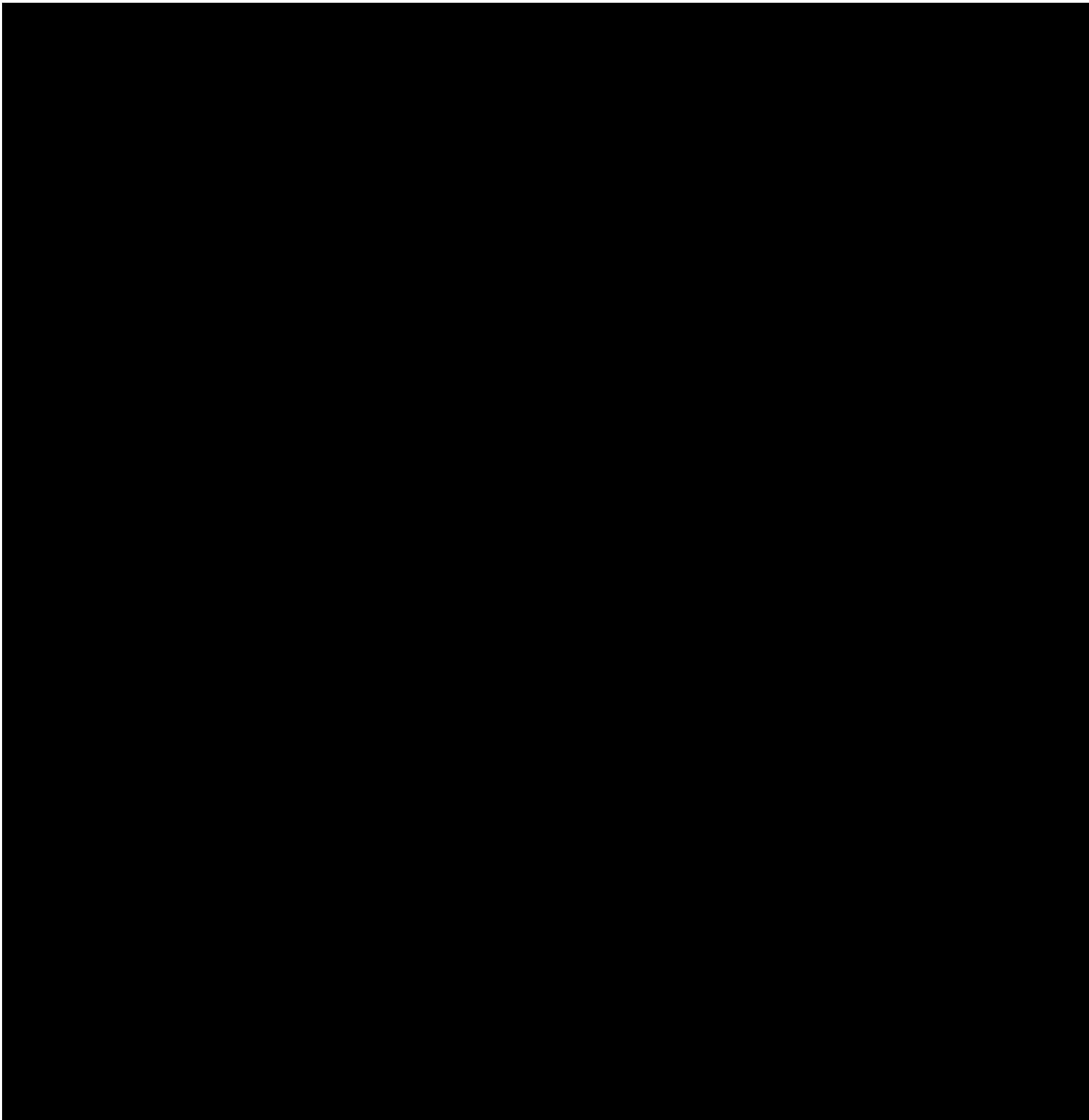
17 August 2020

Bulletin #2020-4334

SINs: NHIAC – 16 | HSEC – 6

(603) 223-3859


NH.IAC@dos.nh.gov



(U) Nationwide - Activity Alert – Malicious Cyber Actor Spoofing SBA’s COVID-19 Loan Relief Website via Phishing Emails - The Cybersecurity and Infrastructure Security Agency (CISA) is currently tracking an unknown malicious cyber actor who is spoofing the Small Business Administration (SBA) COVID-19 relief webpage via phishing emails. These emails include a malicious link to a fake page used for malicious re-directs and credential stealing. Small business owners and organizations at all levels should review the alert and apply the recommended mitigations to strengthen the security posture of their systems.

- [Click here to read the full alert!](#)
- Source: Cybersecurity and Infrastructure Security Agency (CISA)

TLP: GREEN – Not to be shared with the public or media – Nationwide – Personal Protective Equipment (PPE) Fraud Scheme Targeting Healthcare Sector and Utilizing a False FBI Asset Line to Steal Personal Identifying Information (PII) - The Federal Bureau of Investigation (FBI) Baltimore Field Office, in coordination with Office of Private Sector (OPS), prepared this Liaison Intelligence Report (LIR) to inform private sector partners about recent Personal Protective Equipment (PPE) fraud schemes targeting the Healthcare Sector. These schemes involved individuals receiving an email from a broker, who claimed to have access to a vendor with an unlimited supply of nitrile gloves and required potential buyers to contact and provide personal identifying information (PII) to an “FBI Verification Line” as part of the purchasing procedures. With the influx of various vendors selling PPE, it has become more difficult to distinguish fraudulent PPE distributors from legitimate ones. However, FBI asset verification lines do not exist, and the FBI has no role in brokering PPE deals or validating PPE suppliers. During these unprecedented times when organizations are looking to protect their workforce, and medical facilities are seeking to replenish their supplies, opportunists are continuously seeking to capitalize on crucial necessities. In addition to great financial loss, the health and safety of essential front-line workers are at risk due to the purchase of counterfeit products or by PPE not being delivered as promised. These schemes create significant financial and physical safety vulnerabilities for medical professionals, medical facilities, the general public, and pandemic victims.

- Source: Federal Bureau of Investigation 

New Hampshire Information & Analysis Center – COVID-19 Daily Report

(U) INTERNATIONAL

(U//SBU) Not to be shared with the public or media – Nationwide - *ADMINISTRATIVE REVISION: Global Partners' Response to Russian and Chinese COVID-19 Disinformation, May – June 2020* - A compilation of press reporting and government reports suggests that Russia and China continue to conduct COVID-19 pandemic-related malign influence and disinformation campaigns targeting US and global audiences. These narratives continue to deflect criticism and blame, raise doubt about the origin of the virus, inaccurately mischaracterize Chinese and Western government responses, spread conspiracy theories and false health information, and portray Western governments as failures.

- Source: Department of Homeland Security 